Response to Examination of US patent application No. 10/511775 by Aravind K. Moorthy

Steve Moyle, 6th November 2008

Version 1.0

1. *Comments regarding the Vaidya Patent*

Vaidya's 2001 patent "Dynamic Signature Inspection-Based Network Intrusion Detection"

The invention described uses a database of attack signatures built from previously seen attacks. Each access to a computing recourse (or object) is checked against all of the signatures in a "virtual processor". The invention includes the ability to dynamically update the attack signature database at run time. The word "dynamic" refers to threshold numbers of events in periods of time (claim 3).

Vaidya's signatures relate to specific attack attempts whilst Heasman & Moyle relate to entire families of attack attempts.

The signatures: are "rules based", "descriptive of a pattern which constitutes a known security violation". The invention is described as a "dynamic signature-based" including "multiple attack signature profiles which are each descriptive of identifiable characteristics". The "identifiable characteristics" are associated with "**particular** network intrusion attempts". From Claim 3 "attack signature profiled configured to recognize an occurrence of a predetermined number of events within a predetermined time interval". Clearly, these characteristics are related to **particular** previously seen attempts that are then codified into signatures and their rates of occurrence used to trigger actions.

The Heasman & Moyle invention refers to encoding a whole **class** or **family** of intrusion attempts through the means of **semantic specification of attack strategies**. A single attack strategy may give rise to a multitude of different particular attempts (for which Vaidya would require a signature for each of the multitude). The upper bound on the number of particular attacks stemming from a semantic attack strategy is infinite.

Vaidya's signature profiles do not relate to operational semantics of the computing object

Vaidya's step 50 (page 6) of generating signature attack profiles is solely related to simple propositional 'features' of the computing object. E.g. "which network objects are not permitted to access other network objects". The 'feature' based signatures are unable to encode the full operational semantics of the computing object that is being attacked. However, Heasman & Moyle use the full operational semantics as the basis for forming the specification of detectable attack strategies.

The "more formal description of an attack signature" provided on page 10 does not include a way to express the operational semantics of the Network Object. It clearly does not provide a way of

encoding an **attack strategy** or **a family of particular attacks**. There is no use of First Order Logic to express an **attack strategy**.

Vaidya does not claim any automatic learning of "signatures"

Claim 3 relates to "generating an additional attack signature profile configured to recognize an occurrence of a predetermined threshold number of events within a predetermined time interval". The actual "recognition of occurrence" is not learned but rather provided manually in a signature.

Heasman & Moyle learn general rules from examples of events.

2. *Comments regarding the Wrobel Patent*

Wrobel's invention, the MIDOS algorithm, is a method for "discovering groups of objects having a selectable property from a population of objects" from a data base. The invention and its described examples refer to the "sub-division" of data.

Wrobel produces sub-divisions of input data

Wrobel's MIDOS produces "interesting" sub-groups or "sub-divisons" of the data in the data base. Heasman & Moyle do not produce "sub-divisions" rather their invention produces generalisations as **semantic rules** (relating to attack strategies).

Static data in tuples versus sequence data

The input to Wrobel's MIDOS relates to static tuples or "records held in tables" in data bases. Heasman & Moyle use **sequences of elements** (e.g. Intel micro processor instructions).

Operational semantics as background knowledge

Wrobel uses predominately extensional tuples for background knowledge, while Heasman and Moyle use a **program to encode the operational semantics** of the resource being protected (e.g. an Intel microprocessor) for background knowledge which is beyond the capability of MIDOS.

3. *Comments regarding the Bratko & Muggleton's CACM article*

This 1995 background paper "Applications of Inductive Logic Programming" covers a range of problems that had been solved with early ILP techniques up to 1995. None of the applications relates to computer security. None of the applications described relate to encode operational semantics. At that time the ILP techniques (e.g. MIDOS from Wrobel) were unable to deal with the problem domain tackled by Heasman & Moyle.